SEARCH NOTES

09/702,728

WEST Search History

DATE: Friday, November 21, 2003

Set Name side by side	**Query**	**Hit Count**	**Set Name** result set
DB=USPT; PLUR=YES; OP=OR			
L24	L23 and l22	48	L24
L23	(deny$ or reject$ or block$ or disapprov$ or prohibit$ or prevent$ or inhibit$ or restrict$ or limit$) near9 (transaction or purchas$ or buy$)	12933	L23
L22	L21 and l19	70	L22
L21	L20 same l2	3910	L21
L20	track$ or monitor$ or screen$ or review$	969854	L20
L19	L18 and l17	139	L19
L18	payment near7 (summary or history or record)	1039	L18
L17	(prevent$ or reduc$ or avoid$ or lower$ or inhibit$ or prohibit$) near7 (fraud$ or delinquen$)	2768	L17
L16	L15 and l14	10	L16
L15	(flag$ or identif$ or determin$ or record$ or notify$ or notified) near7 (bad$ or fraud$ or delinquen$) near5 account	124	L15
L14	L13 and l12	184	L14
L13	@ad<20001101	3091261	L13
L12	L11 and l9	188	L12
L11	L10 near9 l4	6960	L11
L10	(reject$ or deny$ or disapprov$ or restrict$ or limit$)	2318265	L10
L9	L8 and l7	267	L9
L8	(over or exceed$ or insufficient$ or overdraw$) near7 (limit or funds or amount)	187694	L8
L7	L6 and l3	587	L7
L6	L5 near9 l4	6706	L6
L5	record or summary or history	2398167	L5
L4	transaction or purchas$ or buy$	199907	L4
L3	L2 and l1	988	L3
L2	(credit or debit or bank$ or loan or debt or finanical) near7 (card or account)	20089	L2
L1	(late or fraud$ or bounce$ or history or summary or record or delinquen$)near9 payment	1435	L1

END OF SEARCH HISTORY

WEST Search History

```
DATE:  Friday, November 21, 2003
```

Set Name side by side	**Query**	**Hit Count**	**Set Name** result set
DB=USPT; PLUR=YES; OP=OR			
L16	L15 and l14	10	L16
L15	(flag$ or identif$ or determin$ or record$ or notify$ or notified) near7 (bad$ or fraud$ or delinquen$) near5 account	124	L15
L14	L13 and l12	184	L14
L13	@ad<20001101	3091261	L13
L12	L11 and l9	188	L12
L11	L10 near9 l4	6960	L11
L10	(reject$ or deny$ or disapprov$ or restrict$ or limit$)	2318265	L10
L9	L8 and l7	267	L9
L8	(over or exceed$ or insufficient$ or overdraw$) near7 (limit or funds or amount)	187694	L8
L7	L6 and l3	587	L7
L6	L5 near9 l4	6706	L6
L5	record or summary or history	2398167	L5
L4	transaction or purchas$ or buy$	199907	L4
L3	L2 and l1	988	L3
L2	(credit or debit or bank$ or loan or debt or finanical) near7 (card or account)	20089	L2
L1	(late or fraud$ or bounce$ or history or summary or record or delinquen$)near9 payment	1435	L1

```
END OF SEARCH HISTORY
```

```
?show file;ds
File  15:ABI/Inform(R) 1971-2003/Nov 20
         (c) 2003 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2003/Nov 19
         (c) 2003 Resp. DB Svcs.
File 610:Business Wire 1999-2003/Nov 21
         (c) 2003 Business Wire.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 275:Gale Group Computer DB(TM) 1983-2003/Nov 20
         (c) 2003 The Gale Group
File 476:Financial Times Fulltext 1982-2003/Nov 21
         (c) 2003 Financial Times Ltd
File 624:McGraw-Hill Publications 1985-2003/Nov 20
         (c) 2003 McGraw-Hill Co. Inc
File 636:Gale Group Newsletter DB(TM) 1987-2003/Nov 20
         (c) 2003 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2003/Nov 21
         (c) 2003 The Gale Group
File 613:PR Newswire 1999-2003/Nov 21
         (c) 2003 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File  16:Gale Group PROMT(R) 1990-2003/Nov 20
         (c) 2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2003/Nov 21
         (c)2003 The Gale Group
File  20:Dialog Global Reporter 1997-2003/Nov 21
         (c) 2003 The Dialog Corp.
File 625:American Banker Publications 1981-2003/Nov 21
         (c) 2003 American Banker
File 268:Banking Info Source 1981-2003/Nov W2
         (c) 2003 ProQuest Info&Learning
File 267:Finance & Banking Newsletters 2003/Nov 20
         (c) 2003 The Dialog Corp.

Set     Items   Description
S1    1004960   (CREDIT? OR FINANCIAL OR LOAN? OR DEBT?)(7N)(CARD OR ACCOU-
             NT OR ACCOUNTS)
S2      69545   PAYMENT?(7N)(HISTORY OR HISTORIES OR REPORT? OR SUMMARY OR
             SUMMARIES)
S3      12606   S1 AND S2
S4     734398   CREDIT?(7N)(ACCOUNT OR ACCOUNTS OR CARD)
S5      10225   S4 AND S2
S6      69143   TRANSACTION?(7N)(HISTORY OR HISTORIES OR ACCOUNT OR SUMMARY
              OR SUMMARIES)
S7       1111   S5 AND S6
S8      52032   (BAD? OR LATE?)(7N)PAYMENT?
S9        117   S7 AND S8
S10    152288   (OVER OR EXCEED?)(7N)LIMIT?
S11        14   S9 AND S10
S12     70724   OUTSTANDING(7N)BALANCE?
S13         2   S11 AND S12
S14   9268777   TRACK? OR REVIEW? OR MONITOR?
S15     36451   S14(S)S4
S16      1085   S15 AND S8
S17       258   S16 AND S10
S18     54115   (REJECT? OR DISAPPROV? OR PREVENT?)(7N)(PURCHAS? OR BUY? OR
              TRANSACTION?)
S19         6   S18 AND S17
S20    117623   S2 OR S8
S21     18951   S20 AND S4
S22    733203   FRAUD? OR DELINQUEN?
S23      5295   S22 AND S21
S24       148   S23 AND S18
S25        24   S24 AND S10
S26  14994880   PD<000111
```

```
S27          1   S26 AND S25
S28          8   S26 AND S24
S29      24978   (REJECT? OR DENY? OR DISAPPROV?)(7N)(TRANSACTION? OR PURCH-
             AS? OR BUY?)
S30        132   S15 AND S29
S31          6   S30 AND S10
S32          1   S31 AND S26
S33      30861   15 AND S20
S34       1210   S33 AND S10
S35        106   S34 AND S12
S36         20   S35 AND S26
S37     100540   (LATE? OR BOUNCE? OR BAD? OR FRAUD? OR DELINQUEN? OR HISTO-
             RY OR HISTORIES OR SUMMARY OR SUMMARIES)(9N)PAYMENT?
S38        236   S37 AND S4 AND S29
S39         19   S38 AND S26
?
```

WEST

□ Generate Collection Print

L16: Entry 3 of 10 File: USPT Apr 4, 2000

DOCUMENT-IDENTIFIER: US 6047268 A
TITLE: Method and apparatus for billing for transactions conducted over the internet

Application Filing Date (1):
19971104

Brief Summary Text (4):
On-line transactions between consumers and merchants on the World Wide Web (WWW) are becoming increasingly more numerous as the public becomes more facile in making purchases on the Internet. Such transactions can be for the purchase of "soft" goods, i.e., information, software and other material available in electronic form that can be delivered in real time to a user's client terminal. Such transactions can also be for the purchase of conventional "hard" goods, where the purchased merchandise are delivered off-line. Conventional on-line payment options generally involve the use of credit cards wherein the user provides his or her credit card number on-line or off-line to the merchant provider to pay for the "hard" or "soft" purchase to be delivered on-line or off-line.

Brief Summary Text (5):
Where the transactions involve a relatively small cost, for example $10 or less, the credit card system of payment is too expensive. Further, the credit card payment system excludes potential customers who do not have a credit card, or those who do but do not "trust" either providing their credit card number on-line, or do not want to use their credit card for such purchases. It would be advantageous, therefore, that some trusted transaction intermediary perform the functions of authenticating a user on the WWW and authorizing the transaction. Once such a transaction intermediary authenticates the user and authorizes the transaction, the merchant is alerted to provide the goods or services which are the subject of the transaction and an account associated with the user is billed for the transaction amount. Advantageously, once the user has registered with the transaction intermediary, no sensitive billing information, such as a credit card number, needs to be sent to the merchant.

Brief Summary Text (6):
In co-pending application Ser. No. 08/532,336 filed Sep. 22, 1995 by Y. Ronen, co-inventor herein, and assigned to the same assignee as the present application, a method of billing for services and/or goods ordered over the Internet from a merchant is disclosed. As described therein, the customer/user places a real or a virtual telephone call to the merchant's 900 telephone number and is charged by the telephone company an amount for that call that is representative of the cost of the goods or services being ordered via the Internet from the merchant's server. The merchant's server associates the 900-number telephone call with the request via the Internet for the goods or services in order to authenticate and authorize the transaction. In co-pending patent application Ser. No. 08/636,109 filed Apr. 22, 1996, co-invented by the same Mr. Ronen who is co-inventor herein, and assigned to the same assignee as the present application, a method of billing for transactions conducted over the Internet is disclosed in which a billing server connected on the Internet receives the IP address assigned to that user's client for the current user session and an indication of the user's identity from the user/customer's Internet Access Provider (IAP). In response to a chargeable transaction, the merchant's server transmits to a billing platform the IP address identity of the user making the transaction and the cost associated with the transaction. The billing server then cross-references the IP address associated with the cost of the transaction received from the merchant's server with the IP-address/user-identity relationship received from the IAP to

properly charge an established account of the user for the transaction. Such an account is established by the user prior to the execution of the transaction for billing in a predetermined manner to, for example, the user's selected credit card, the user's debit card, the user's telephone account associated with his or her phone number, the user's merchant credit card, or other billing mechanism. For this billing methodology, arrangements thus need be established between billing server and the large number of different Internet Access Providers that provide Internet access to a tremendously large customer base since for each user's session the IAP must be programmed to forward to the appropriate billing server the relationship between the user's currently assigned IP address and identity.

Brief Summary Text (9):
A subscribing user who has registered with the provider of the billing system of the present invention may browse the home page of a merchant which has itself made previous arrangements with the provider of the billing system. While "visiting" the merchant's site, which has also registered with the billing system, the subscribing user is offered the option to purchase some good or service at a stated price for either on-line or off-line delivery. In response to the user's intent to purchase the selected item and be billed via the billing system, the merchant's digitally signed order is sent to the billing system for authentication and authorization of the transaction. Specifically, in accordance with the present invention, information previously provided to the user's client terminal's cookie file is transmitted to a billing server within the billing system. This information comprises a static information portion and a transaction oriented dynamic information portion, which are encrypted prior to transmission. The static information portion identifies the user through an assigned account number. The transaction oriented dynamic information portion comprises at least one sequence that was sent to the user's cookie file by the billing server upon a previous transaction, and is valid for only a single new transaction. The billing server, upon receiving from the user's browser program the cookie containing the encrypted static and dynamic information portions and decrypting same, identifies the user from the static portion, and accesses from an associated database the expected transaction oriented dynamic portion that the billing server last sent to that user. If the expected dynamic portion matches the received dynamic portion, the user is authenticated to proceed with the current transaction. The billing server, upon authentication of the user, then authorizes the specific transaction based on various criteria such as the user's credit limit, the cost of the transaction, etc. The billing server then sends to the user's browser a new cookie which contains the user's account identity in the static information portion and a new transaction oriented dynamic portion to be used by the user's browser for authentication of the user for a next transaction. Upon receipt, the user's browser program installs the new cookie and provides the user the opportunity to reject or finally approve of the transaction. If approved by the user, the order is sent to the merchant's server via the user's client terminal browser program. Upon receipt, the merchant's server posts the complete transaction information to the billing server for billing and provides for the delivery of the goods or services to the user. The customer's transaction is then confirmed through an acknowledgment sent via e-mail transmitted to the e-mail address associated with the account number. The billing server either after each transaction, or on a periodic basis, sends the transaction summary to a billing platform for billing of the user based on his or her registered billing preference such as a telephone bill, credit card charge, or a direct invoice. The billing platform then settles with the merchant after a fixed number of days, contingent on the user paying his or her bill.

Detailed Description Text (2):
With reference to FIG. 1, a user at a client terminal 101 is connected to the Internet 102 through an Internet Access Provider 103. The connection between the client terminal 101 can be, for example, through a Local Exchange Carrier (LEC) (not shown), through a cable TV network (not shown), or through another access medium. The client terminal 101 could also be connected directly to a Local Area Network which is directly connected to the Internet 102. The client terminal 101 runs a browser program which enables the user to "surf the Net" to visit various sites connected to the Internet. Some of these sites only provide information content and other sites may provide information in conjunction with offers of services and/or "soft" or "hard" goods with an associated cost. The services for a fee may include the delivery to the user of information itself, or the delivery of "soft" goods that can be delivered

digitally on-line over the Internet to the client terminal, such as software, music, video, etc. If the user orders "hard" goods over the Internet, as for example clothing, delivery need obviously be made off-line. Some of these transactions that involve the delivery of information or a software program may have a relatively low cost to associated with them. Further, a user may visit such an on-line merchant's site only once or very infrequently. The present invention eliminates the need for the user to establish a financial relationship with the on-line merchant who is supplying the soft or hard goods that are the subject of the transaction. Thus, the user need not provide any financial information, such as a credit card or other personal information to the merchant to be assured initiation of the delivery process for the desired soft or hard goods or services. Accordingly, a user who has registered with the billing system 104 of the present invention and who enters into an on-line transaction with a registered merchant can obtain the transacted-for hard or soft goods or services without having to provide any personal information to the merchant, including his or her identity. The merchant, having registered itself with the billing system, can also be assured of receiving payment from the trusted provider of the billing system since it knows that each transaction will be user-authenticated and authorized by the billing system.

Detailed Description Text (3):
In order to conduct on-line transaction through the billing system 104, the user needs to register with the system. This registration occurs at the user's initiative, by posting information via the Internet to a registration server 105 within billing system 104 or by paper (e.g., fax or mail), or by telephone. The registration process occurs once per user. The process allows a user to establish an account, which requires a billing name, address, e-mail address, and billing preferences for charges made to the account. The latter may include a direct bill to an email address or to the postal address associated with the user's telephone number, or to a telephone bill (LEC or Interchange carrier), or to a user's credit card or debit card. These preferences can be distributed amongst different billing mechanisms as a function of the type of transaction being billed. Thus, the user can direct that all transactions of less than a predetermined cost be billed to his or her telephone bill, and those of greater than that cost be billed to his or her credit card. Also, the user can direct transactions of a certain type, such as purchases of software to be direct-billed and other types be billed according to the cost of the goods as noted above. Other information unique to the user, such as a password, is also obtained in the registration process that can be later used to validate the billing information. The information can be updated when the user's billing information changes, or additional users need to added/removed from an specific account. If entered on-line through registration server 105, the information is stored in a database 106 for later retrieval. If received from the user by another methodology, the information is entered by an operator associated with the billing system 104 and stored in database 106.

Detailed Description Text (13):
Assuming that the user has been authenticated, the transaction needs to be authorized by the billing system. When the user "clicks-to-buy", which is the stage in the merchant-user electronic shopping web interface when the user has confirmed a willingness to complete the transaction with the stated terms, the transaction must be authorized. The order information, digitally signed by the merchant is sent through the user's client terminal's browser to the billing system 104. The order amount, combined with the cookie file containing the user's account ID number and transaction number, provide sufficient information to query the user's profile stored in database 106 to verify if the transaction should be authorized. Authorization for the transaction will be granted if (1) the user is registered as active in the billing system; (2) the merchant is registered with the billing system; (3) the user is not blocked from making purchased based on payment history; (4) the purchase amount does not exceed a per-transaction limit specified by the user upon registration; (5) the purchase amount does not exceed the billing system's specified cumulative credit limit; and (6) the purchase does not violate any customer-specified restrictions (e.g., block transactions during certain times) or preferences (e.g., block transactions for certain types of merchandise). If authorization is denied, a message is displayed on the user's browser indicating that the purchase cannot be authorized and inviting the user to contact a customer assistance representative at a specified phone number. Additional criteria can also be used to determine whether or not to

authorize a specific transaction.

Detailed Description Text (16):
At the end of the user's Internet session, or periodically if there is any activity related to the user's account, the billing system transmits an email summary to the account holder showing all the transactions conducted over a period of time. The information provided shows the transaction ID, the amount, date/time of purchase and merchant name.

Detailed Description Text (18):
At step B208, a determination is made whether the transaction is authorized. To do this, the encrypted message containing the original order, the merchant's signature and the certificate are decrypted. The billing system then determines whether the transaction can by authorized. As previously noted, a transaction is authorized if the user is registered in the billing system database, the merchant is registered with the billing system, the user is not blocked from making purchases based on payment history, the purchase amount does not exceed a per-user specified limit, and the purchase does not violate any customer-specified restrictions or preferences. If the transaction is not authorized, at step B209, a message is returned to the merchant through the user's browser indicating that the transaction was unable to be authorized. At step C206, the user receives the message with directions to call a specified customer assistance number for further information.

CLAIMS:

15. The method of claim 10 further comprising:

if the received password does not match a stored password associated with the user's account number, denying the transaction.

16. The method of claim 8 further comprising:

if the transaction-oriented dynamic information portion in the transition-oriented received cookie does not match the stored transaction-oriented dynamic information portion, denying the transaction.

17. The method of claim 13 further comprising:

if the transaction-oriented dynamic information portion in the received cookie does not match the stored transaction-oriented dynamic information portion, determining whether any fraudulent transactions were made on the user's account.

WEST

□ Generate Collection Print

L24: Entry 45 of 48 File: USPT Jun 25, 1996

DOCUMENT-IDENTIFIER: US 5530438 A
TITLE: Method of providing an alert of a financial transaction

Brief Summary Text (4):
Credit and debit accounts of various sorts have permeated today's financial environment. It is a matter of convenience for holders of these accounts to pay for goods and services or conduct financial transfers by presenting the appropriate account card or account number to the provider of such goods and services. The foregoing is done with the understanding that they will be billed for the sale amount at a later date, or that their accounts will be immediately updated to reflect the transaction. The need to carry money or have a sufficient amount of money available in a checking account is no longer required. In order to obtain credit accounts, one must generally have a proven, reliable credit history which is devoid of past due payments to creditors.

Brief Summary Text (9):
In the past, credit issuers and providers of goods and services have taken some steps to protect themselves from such fraud. Prior art techniques involve on-line credit checks at the point of sale; i.e., electronic access to off-site databases to determine whether the credit account being used by a purchaser is valid, or if cards issued under that account have been reported lost or stolen by the account owner or cardholder. This approach prevents fraudulent use of the victim's illicitly obtained (e.g., lost or stolen) cards only after the victim reports the loss/theft to the issuing organization. As mentioned earlier, the victim may not be aware of the loss immediately, so the cards can be easily used by the perpetrator until such time that the loss is reported.

Brief Summary Text (11):
In addition to the aforementioned, some account issuers monitor account activity in real-time and compare present activity with historic patterns of use for that cardholder. This is done in an attempt to identify suspicious activity indicative of fraudulent use, and to deny transactions in such instances. Of course, this technique is subjective in nature and might therefore lead to improper occurrences of both denial of legitimate transactions and approval of fraudulent transactions. Account issuers also offer credit protection plans, however such plans only limit the victim's liability, but do not prevent fraudulent transactions from occurring. Neither of these practices are capable of protecting victims from activity on unauthorized accounts, opened under a victim's name and social security number, when the victim is unaware of these accounts.

Brief Summary Text (13):
Accordingly, there exists a need to effectively combat the problem of consumer account fraud. A solution capable of alerting the point of sale provider of goods and services, the relevant financial institution, and the potential victim to an impending fraudulent transaction, would be an improvement over the prior art. Further, a method that provides the ability to prevent completion of a fraudulent transaction, in real time (i.e., while it is being attempted), would be quite beneficial.

Drawing Description Text (2):
FIG. 1 shows a simplified block diagram of a financial transaction alerting system, in accordance with the present invention; and

Detailed Description Text (3):

The invention can be better understood with reference to FIGS. 1-2. FIG. 1 shows a simplified block diagram of a system (100) in which an alertable financial transaction occurs, in accordance with the present invention. The system (100) includes at least one radio system (102) that is capable of transmitting messages within a particular coverage area, (i.e., a known paging system might be effectively utilized). Alternatively, two-way wireless communication systems, such as conventional or trunked radio systems, might be used to effectuate and support either one-way or two-way communications, as later described. In addition, the system includes a database (104) that retains information as described herein, and can either be located remotely with respect to the radio system (102), or can be an integral part thereof, depending upon the needs of a particular application.

Detailed Description Text (8):
Having been so alerted, the radio system user (126) might optionally use the radio (128) to review information pertaining to the financial transaction and/or information pertaining to the customer (118), as later described. The radio system user (126) might further use the radio (128) to broadcast a user message (132), which might include a request to approve or disapprove the financial transaction. In this arrangement, the user message (132) is received by the radio system (102) and delivered to the provider (116), who uses the message in deciding whether to complete or deny the financial transaction. The radio system (102) might also measure the time elapsed since the financial transaction message was broadcast and, after a predetermined time, deliver an appropriate message to the provider (116), as later described.

Detailed Description Text (9):
There are, of course, alterations or modifications to the above that can be made. For example, information regarding one or more physical characteristics of the customer (118) might be obtained by the provider (116) and made a part of a message (129) that is transmitted to the radio system user authorized to conduct the financial transaction (126). Such information might be automatically provided in a variety of ways, such as a finger print reader, retinal eye scanner, digital photography, voice sampling, etc. The physical characteristic information might also be entered by the provider (116) after making a personal observation of the customer (118). It should be noted that, to facilitate the above, it may be necessary to provide a more highly featured radio (128, 130). For example, to display a digitized photograph of the customer (118) the radio (128, 130) would either need an integral display capability or otherwise be provided with some means of transferring that information to another display medium. Such physical characteristic information, when provided to the radio system user authorized to conduct the financial transaction, provides an additional layer of protection that can be effectively used to adequately prevent illicit financial transaction activities.

Detailed Description Text (13):
Use of a timer (213) is contemplated as follows: when a user message pertaining to the financial transaction is not received before the timer expires, the financial transaction may be completed or denied (217), in accordance with a predetermined arrangement made by the person authorized to conduct the financial transaction. In this manner, the authorized user might arrange to enable completion of only those transactions that are positively approved (e.g., by a response signal transmitted to the radio system). Similarly, an arrangement can be made that approves all transactions that are not specifically disapproved within a certain time. Further, if the identified person(s) are not radio system users, a message indicative of this fact might be sent to the goods/services provider.

CLAIMS:

23. The method of claim 21, wherein when the user message comprises a disapproval, the step of using the user message to further direct the financial transaction includes the step of denying completion of the financial transaction.

32/9/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00576649 91-50996

Processing Credit Cards

Kasavana, Michael

Restaurant Business v90n15 PP: 94 Oct 10, 1991 ISSN: 0097-8043
JRNL CODE: RTB
DOC TYPE: Journal article LANGUAGE: English LENGTH: 1 Pages
WORD COUNT: 787

ABSTRACT: It is to a restaurant operator's advantage to facilitate payment by credit card. Customers appreciate the option, and the convenience often encourages freer spending. There have been 2 important developments in restaurant automation: electronic data capture (EDC) and online credit-card authorization (CCA). EDC is primarily concerned with the rapid recording and storage of credit card information. Online CCA involves instantaneous validation and settlement processing of credit card transactions. Manual data gathering procedures are being replaced by magnetic stripe readers. Online CCA provides effective protection against fraudulent credit card use. In an arrangement involving an independent transactional processing technology system, a terminal with EDC and CCA capabilities is placed alongside a point of sale terminal at each cashier position. Debit cards require that a cardholder must have prepaid a purchase or have sufficient funds in a bank account at the time goods and services are received.

TEXT: Customers appreciate the option of paying by credit card to defer payment. And, the convenience of a credit card often encourages freer spending. So, it is to the operator's advantage to facilitate payment by credit card. The challenge is to determine the most effective means of processing them.

Two of the most important developments in restaurant automation have been electronic data capture (EDC) and online credit-card authorization (CCA). EDC is primarily concerned with the rapid recording and storage of credit-card information. CCA involves instantaneous validation and settlement processing of credit-card transactions.

PROCESSING CYCLE. Historically, cashiers had to manually record **credit - card** data onto **credit - card** vouchers. During the course of settlement, the cashier was required to **review** "bad card" lists or telephone an authorization "hot line" for company approval. Manual data gathering procedures are being replaced by magnetic stripe readers. The cashier passes the **credit card** through a stripe reader to capture the cardholder number and expiration date. This is often tied to a telephone interface to a computer data base for authorization. The authorization process validates the cardholder's **account** data and endorses the **transaction** .

Computerized credit- **card** authorization systems approve or **reject credit - card transactions** within a matter of seconds. On-line credit-card authorization provides effective protection against fraudulent credit-card use.

In a CCA system, an EDC terminal reads the credit-card number and expiration date coded on the magnetic stripe on the back of the card and instantaneously dispatches an authorization request. The call typically goes out to a bank or a consortium designed to consolidate financial information from several data bases. Credit authorization can be conducted on at least two levels of investigation. Some automated schemes simply check the card's account number against a list of lost, stolen, or otherwise invalid cards; if a match is found, authorization of the transaction is denied.

More comprehensive authorization involves the determination of whether a valid card has **exceeded** its credit **limit** . A thorough check involves examining the customer's actual credit file, typically stored in a data base maintained by the bank that issued the card or a processing-center consortium. By adding the transactional total to the outstanding credit-card account balance and comparing the new total with the credit limit, the system determines whether the transaction should be allowed. If the transaction is endorsed, an authorization code is generated and the new account balance is stored in the data base so that the next credit check will be made against current data.

CONSIDERATIONS. Should the **credit - card** authorization process be a part of the point of sale system or a separate stand-alone system? This question has led some vendors to develop independent transactional processing technology (TPT) systems. In a TPT arrangement, a terminal with EDC and CCA capabilities is placed alongside a POS terminal at each cashier position. The TPT terminals are networked to a central TPT station responsible for data collection and **monitoring** of **credit - card** activity. Proponents of TPT schemes claim they minimize the number of phone lines necessary to support multiple cashier station calls, while contributing to an enhanced cash-flow cycle for the restaurant.

A recent development is the introduction of debit-card technology. While credit cards allow cardholders to receive goods and services first and pay later, debit cards adhere to a pay first, receive products second format.
DEBIT CARDS. A debit card requires that a cardholder must have prepaid a purchase or have sufficient funds in a bank account at the time goods and services are received. In the case of prepayments, debit cards with cash value are purchased in dollar amounts similar to traveler's checks. When the cardholder presents a cash card for transaction settlement, the amount of the transaction is subtracted from the dollar balance of the card.

For example, a $20 card may be presented for a $5 meal. The card's magnetic stripe, which carries the card's remaining balance, would be adjusted to a new balance of $15. Sometime during the day, the restaurant automatically processes all of its debit transactions and the money represented by the transactions is transferred to the business' bank account for immediate use.

Alternately, debit cards can be tied to a cardholder's bank account. When a debit card is presented at the point of sale for transaction settlement, the value of the transaction is electronically transferred from the account of the cardholder to the restaurant's bank account. This electronic funds transfer assures the restaurant of payment and provides instantaneous cash flow.

FUTURE TENSE. EDC and CCA are making a significant impact on the financial strength of the restaurant industry. Soon, however, debit cards may provide an even more pivotal financial opportunity for the foodservice industry.

Dr. Kasavana is a professor at the School of Hotel, Restaurant, and Institute Management of Michigan State University.

THIS IS THE FULL-TEXT.
GEOGRAPHIC NAMES: US

DESCRIPTORS: Restaurants; Credit cards; Automation; Online transaction processing; Authorizations; Bank debit cards
CLASSIFICATION CODES: 9190 (CN=United States); 8380 (CN=Hotels & restaurants); 3200 (CN=Credit management); 5250 (CN=Telecommunications systems)
?

28/9/5 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01210769 SUPPLIER NUMBER: 06084680 (THIS IS THE FULL TEXT)

Amex builds an Expert System to assist its credit analysts; early tests show productivity gains, reduced credit losses as credit risks are more accurately identified. (American Express) (Section 2 Connectivity)

Steinberg, Don

PC Week, v4, n46, pC1(3)
Nov 17, 1987
ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1583 LINE COUNT: 00127

ABSTRACT: American Express has designed an expert system to help its credit authorizers decide when to approve or deny a purchase. The system, called the Authorizer's Assistant, analyzes data from more than a dozen mainframe databases, then presents the authorizer with an approve-deny recommendation and the information that decision was based on. It also produces a screen display that explains the decision. Final authority still rests with the human authorizer, but a three-month study of decisions made with and without the Authorizer's Assistant has shown that far fewer accounts approved by the system end up in the collection department. The speed of the system has improved productivity 20 percent, and American Express expects the system to pay for itself in less than two years. The added savings accrued by fewer accounts going into collection should produce an additional five times the return on investment over the productivity gains.

TEXT:

Amex Builds an Expert System To Assist Its Credit Analysts

Early Tests Show Productivity Gains, Reduced Credit Losses as Credit Risks Are More Accurately Identified

A computerized expert system that draws its conclusions from more than a dozen mainframe databases will soon make it easier for American Express (Amex) employees to live with one of the features that has made the American Express card famous worldwide.

Its lack of a preset spending limit has been critical to the success of the American Express charge card. Unlike bank-issued cards such as Mastercard and VISA, which impose a dollar limit on cardholders, Amex lets members rack up charges as high as they like--as long as they pay the entire bill every month.

However, while this policy is good for customer relations, it can be a headache for many Amex employees. Since there is no defined point at which credit should be denied to a customer, certain employees, called authorizers, must decide whether a purchase will be approved or denied.

Currently, some 200 to 300 authorizers, situated at four U.S. authorization centers, are devoted to the task of making these decisions. Sitting at IBM 3278 terminals, the authorizers receive basic information on a "purchase in progress' and must then toggle among a loosely organized group of mainframe databases, which hold customer credit histories, to determine whether to authorize the purchase.

The process may involve simply checking a customer's recent **payment history** or looking at the bank- **account** information given on the customer's original **credit - card** application. Either way, Amex guarantees its merchants that authorizers will make a decision within 90 seconds.

The cost of making wrong decisions can be huge. If an authorizer **rejects** an attempted **purchase** because the account has an unusually high balance or a **history** of frequent **late payments** , for example, Amex loses the revenue it would collect from the merchant for the transaction and also risks losing the insulted shopper as a member.

Conversely, if the authorizer approves a purchase that should not have been approved, the company faces the risk of never receiving payment. Losses from unpaid bills and **credit - card fraud** are staggering. "It's a nine-digit problem for them [in the hundreds of millions of dollars annually]," said Alex Jacobson, president and CEO of Inference Corp., the Los Angeles artificial intelligence (AI) software developer that Amex called upon to help develop its expert system.

We're Talking Stress

Authorizers don't need to see such numbers to know that their job is rough. "This is a high-pressure job," said Ted Markowitz, director of technology strategy at American Express. "The burnout level is pretty high."

In 1984, Bob Flast, then manager of the credit-authorization department for Amex's American Express Travel Related Services Co. subsidiary in New York, devised a way to use information systems to try to relieve some of the pressure on his staff.

Mr. Flast presented a proposal to build a computerized expert system that would lighten the authorizers' load. The system would condense the array of customer data authorizers need to view during each transaction into a single screenful of data. Using rules garnered through interviews with the company's most experienced authorizers, the expert system also would formulate an approve-or-deny suggestion.

Once the company approved funding for the project, dubbed the Authorizer's Assistant, Mr. Flast recruited Mr. Markowitz to assist him in the system's planning and implementation.

From the beginning, the planners of the Authorizer's Assistant were confident that the project would succeed in the modest goals of increasing the productivity of human authorizers, Mr. Markowitz said. Still, the project did present risks, he said.

AI had never been used at American Express or anywhere else in a credit-authorization application, and the project was being carried out in an environment where success--or failure-- would be obvious, according to Mr. Flast.

Not every American Express card transaction goes to a human authorizer. In fact, 95 percent of them are approved by the firm's Computerized Authorization System (CAS). But that still leaves human authorizers with a large number of decisions (American Express officials declined to provide an exact figure).

The authorization process begins whenever a consumer presents an American Express card to make a purchase, and the merchant contacts American Express to verify that the **card** is valid and the customer is **credit** -worthy (by checking with Amex, the merchant is relieved of responsibility for **fraud**), according to Mr. Flast.

Most merchants contact Amex for authorizations electronically through point-of-sale systems or **credit** - **card** readers. Others dial a toll-free telephone number and read the purchase and card information to Amex personnel.

Most Are Safe

In either case, the information is sent to an IBM mainframe at the company's data center, in Phoenix, Ariz., that runs CAS. CAS is a simple application that uses straightforward statistical analysis to separate normal transactions from those that might pose a problem. About 95 percent of the time, transactions are "system approved' by CAS within four or five seconds, according to Betsy Fearnow, project director of advanced technology at the Phoenix data center.

If CAS's statistical checks reveal potential problems with the transaction due to unusual account activity or a large account balance, Mr. Markowitz said, it refers the decision to human authorizers. Amex officials declined to reveal the parameters that would cause CAS to send a transaction to a human authorizers.

At this point, with the old system, the human authorizer would be sent a screen of data from CAS on the current transaction, and would then need to access more than a dozen separate databases of customer records, synthesizing the information found there in order to make an authorization decision within 90 seconds. The expert system, which was prototyped in 1986 and pilot-tested early this year, is designed to simplify that process.

Authorizer's Assistant includes about 800 rules, some designed to condense customer data, others designed to formulate a recommendation, according to Mr. Markowitz. The expert system presents authorizers with a single screen of information that consists of an approve/reject recommendation and the data upon which that recommendation was based. It also produces a second screen that provides explanations of its decisions, he said. The final approval or rejection decision still rests with a human authorizer, however, he said.

Productivity's Up

From its first test, the Authorizer's Assistant has been a boon to the productivity of Amex's credit authorizers, Mr. Flast said. In the testing that has been conducted with authorizers using the expert system--which now is scheduled to go live in Amex authorization centers beginning next spring--the company has seen a 20 percent increase in productivity, he said.

Based on those productivity gains, American Express expects Authorizer's Assistant to pay for itself in a little less than two years, he said.

"As the number of transactions grows, we won't have to hire as many new people," said Mr. Flast, who is now Amex vice president of corporate technology strategy.

American Express expects its transaction volume to increase significantly thanks to its recently introduced Optima **credit** **card** , which offers a revolving **credit** line similar to those offered by Mastercard and VISA.

There also also indications that other benefits of the new expert system will be much greater than anticipated, Mr. Flast said, with some gains directly affecting the millions Amex loses each year due to **fraud** and bad credit.

For instance, a recent test looked at 2,500 decisions made by authorizers with and without the expert system's help and then checked the quality of the cardmember accounts involved three months later. The study found that in cases where Authorizer's Assistant was used, far fewer accounts ended up in the collections department. Based on these tests, the company expects to cut its number of 90-day-overdue bills (the point at which accounts are referred to the collection department) in half. This benefit, said officials, would produce an additional five times the return on investment from the initial productivity gains.

Planners at Amex attributed success of the project to its use of AI techniques, which have allowed the firm to turn the amassed base of authorization knowledge among its senior authorizers into a hard and retained asset. The leap in performance created by Authorizer's Assistant could only have been brought about by an entirely new technical approach, they said.

Officials hope the expert system will improve consistency in authorizations among the firm's hundreds of authorizers, who vary widely in experience. They also hope the system will reduce the high burnout rate among authorizers.

The project has proven to be a springboard for new AI-related projects all across Amex.

"It was a proof of concept," said Mr. Markowitz. "There are 10 other AI-based systems now in place across the company."

Photo: Bob Flast, an Amex vice president, turned to an expert system as a way of taking pressure off the company's over-burdened credit-approval staff.

Photo: American Express Purchase-Authorization Process with Authorizer's Assistant

CAPTIONS: Bob Flast. (portrait); American Express purchase-authorization process with Authorizer's Assistant. (chart)

SPECIAL FEATURES: illustration; portrait; chart
COMPANY NAMES: American Express Co.--Automation
DESCRIPTORS: Connectivity; Artificial Intelligence; Expert Systems; Credit Authorization
SIC CODES: 7372 Prepackaged software
TICKER SYMBOLS: AXP
FILE SEGMENT: CD File 275

?